The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/06/2020

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in iOS, iPadOS, macOS, tvOS, watchOS, and Safari. The most severe of these vulnerabilities could allow for arbitrary code execution.

- iOS is a mobile operating system for Apple cellphones.
- iPadOS is a mobile operating system for Apple tablets.
- macOS is a desktop operating system for Macintosh computers
- tvOS is an operating system for the Apple media streaming device Apple TV.
- WatchOS is an operating system for Apple watches.
- Safari is a web browser available for macOS.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Successful exploitation of these vulnerabilities could allow the attacker to execute remote code on the affected system.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- iOS prior to 13.6
- iPadOS prior to 13.6
- macOS prior to 10.15.6
- tvOS prior to 13.4.8
- watchOS prior to 6.2.8
- iTunes prior to 12.10.8

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in iOS, iPadOS, macOS, tvOS, watchOS, and iTunes. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2020-9872)
- An out-of-bounds read was addressed with improved input validation. (CVE-2020-9873, CVE-2020-9938)
- A buffer overflow issue was addressed with improved memory handling. (CVE-2020-9919)
- An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2020-9871, CVE-2020-9874, CVE-2020-9879, CVE-2020-9937, CVE-2020-9876)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2020-9877)
- An integer overflow was addressed through improved input validation. (CVE-2020-9875)
- A buffer overflow issue was addressed with improved memory handling. (CVE-2020-9878, CVE-2020-9883)
- A buffer overflow was addressed with improved bounds checking. (CVE-2020-9866)
- A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. (CVE-2020-9862)
- A denial of service issue was addressed with improved input validation. (CVE-2020-9931)
- A logic issues were addressed with improved restrictions. (CVE-2020-9864, CVE-2020-9903, CVE-2020-9911, CVE-2020-9912)
- A logic issue was addressed with improved state management. (CVE-2020-9925)
- A logic issue was addressed with improved validation. (CVE-2020-9870)
- A memory corruption issues were addressed by removing the vulnerable code. (CVE-2020-9865, CVE-2020-9907)
- A memory corruption issue was addressed with improved memory handling. (CVE-2020-9923)
- An access issue existed in Content Security Policy. (CVE-2020-9915)
- An authorization issue was addressed with improved state management. (CVE-2020-9933)
- An input validation issue existed in Bluetooth. This issue was addressed with improved input validation. (CVE-2020-9914)
- An input validation issue was addressed. (CVE-2019-19906)
- An issue existed in the handling of environment variables. This issue was addressed with improved validation. (CVE-2020-9934)

- An issue existed in the handling of iMessage tapbacks. The issue was resolved with additional verification. (CVE-2020-9885)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2020-9799, CVE-2020-9888, CVE-2020-9890, CVE-2020-9891, CVE-2020-9909)
- An out-of-bounds read was addressed with improved input validation. (CVE-2020-9894, CVE-2020-9918)
- An out-of-bounds write issues were addressed with improved bounds checking. (CVE-2020-9884, CVE-2020-9889, CVE-2020-9936)
- A routing issue was addressed with improved restrictions. (CVE-2019-14899)
- A URL Unicode encoding issue was addressed with improved state management. (CVE-2020-9916)
- A use after free issue was addressed with improved memory management. (CVE-2020-9893, CVE-2020-9895)
- A remote attacker may be able to cause arbitrary code execution (CVE-2019-20807)
- A remote attacker may be able to cause a denial of service (CVE-2020-9917)
- A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication (CVE-2020-9910)
- Vulnerability may allow a remote attacker to cause arbitrary code execution. (CVE-2019-20807)
- Vulnerability may allow local user to leak sensitive user information (CVE-2020-9913)
- An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. (CVE-2020-9900)
- A local user may be able to load unsigned kernel extensions. (CVE-2020-9939)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Successful exploitation of these vulnerabilities could allow the attacker to execute remote code on the affected system.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Apple:

https://support.apple.com/en-us/HT211288

https://support.apple.com/en-us/HT211293
https://support.apple.com/en-us/HT211289
https://support.apple.com/en-us/HT211290
https://support.apple.com/en-us/HT211291

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9512
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14899
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19906
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9799
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9854
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9862
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9863
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9864
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9865
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9866
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9868
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9869
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9870
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9871
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9872
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9873
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9874
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9875
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9876
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9877
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9878
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9879
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9880
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9881
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9882
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9883
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9884
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9885
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9888
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9889
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9890
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9891
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9892
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9893
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9894
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9895
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9899
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9900
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9901
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9903
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9904
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9905
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9906

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9907
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9908
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9909
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9910
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9911
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9913
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9914
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9915
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9916
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9917
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9918
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9919
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9920
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9921
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9923
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9924
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9925
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9927
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9928
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9929
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9931
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9933
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9934
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9936
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9937
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9938
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9939